(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 063 627 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
27.12.2000 Bulletin 2000/52

(51) Int Cl.[7]: **G09F 3/03**

(21) Application number: **00305269.3**

(22) Date of filing: **22.06.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.06.1999 GB 9914711**

(71) Applicants:
- **Leck, Michael John**
  Goostrey, Cheshire CW4 8JR (GB)
- **Mason, John Edward**
  Tarporley, Cheshire CW6 9DE (GB)

(72) Inventors:
- **Leck, Michael John**
  Goostrey, Cheshire CW4 8JR (GB)
- **Mason, John Edward**
  Tarporley, Cheshire CW6 9DE (GB)

(74) Representative: **W.P. Thompson & Co.**
Coopers Building,
Church Street
Liverpool L1 3AB (GB)

(54) Electronic seal, methods and security system

(57) An electronic seal (2) is disclosed which comprises a housing (4,104) and a closure member cooperable with the housing to form a seal. The closure member may for example take the form of an elongate member (6,106) connectable at both of its ends to the housing. The closure comprises an outer portion (8,108) surrounding a core (10,10A,110). Means (14,16,135,136) are provided for sensing integrity of the core. Hence tampering with the seal can be detected. The core may be formed as a fibre optic cable (10,10A) with integrity sensing means comprising an optical source 14 and an optical detector 16.

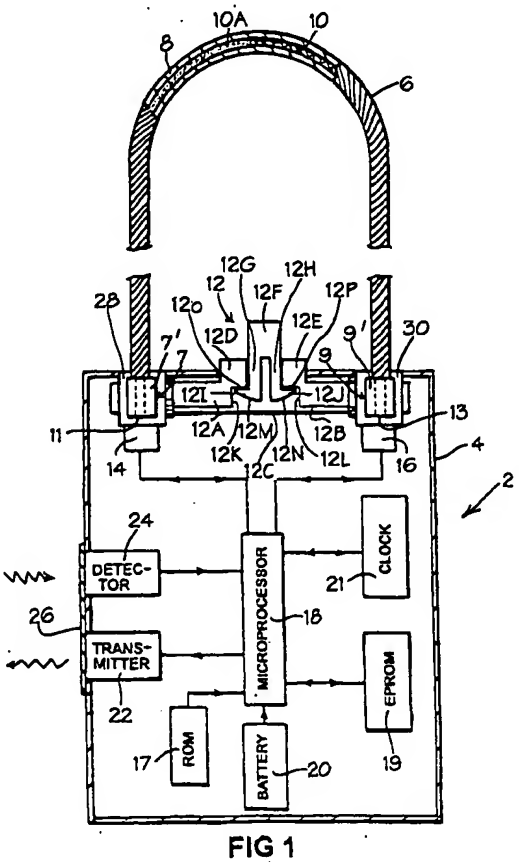

FIG 1

EP 1 063 627 A2

Description

[0001] The present invention relates to an electronic seal capable of monitoring its own security state, for example an electronic seal for securing in a closed position a door or other closure closing an aperture allowing access to an enclosed space (e.g. a container). The invention also includes a seal capable of communicating with a reading and/or programming device.

[0002] The invention also relates to a method of sensing the security status of an electronic seal and a method of communication.

[0003] The present invention also relates to an electronic security system including such a seal. The invention also includes a reading and/or programming device suitable or adapted to communicate with such a seal.

[0004] There exists a need to monitor the security status of cables, bands or other elongate members which form a loop or other connection either of themselves or when one or both ends thereof are fixed to a lock or seal. In particular, if the continuity integrity of the loop, connection or elongate member is broken by tampering, e. g. by cutting the cable, band etc. or by releasing the cable from the lock/seal, then there is a need to detect this.

[0005] Various solutions to this problem have been proposed. For example, a recently publicised "electronic tag" for criminals (The Times 29th January 1999) emits coded electric pulses every few seconds by radio frequency. If the securing strap is broken or tampered with, an alert code is transmitted to the monitor which sends an alarm to a control station. If the tag moves out of range of a monitor, an alarm is also sent to the control station.

[0006] The Crypta III device marketed by Encrypta Electronics Ltd. UK and described in publications EP 0,193,297 Al and B1 monitors the receipt and release of the releasable end of a security cable into/from a recess in a housing. A random code generated by the receipt or release is displayed via an LED. However, this device cannot detect its cable being cut.

[0007] There are numerous electronic seals (for example, Electronic Seal PTE Ltd, Singapore; Sealtronic SA, Switzerland) which check for electrical continuity of a standard steel rope or cable. Tampering is assumed to break the electrical continuity of a steel security cable. However, it is believed that the circuit could be kept intact with a simple shunt cable while cutting the security cable, in which case the tampering would probably not be detected by the seal. Information is transmitted by radio frequency.

[0008] An application note published in 1992 by Dallas Semiconductor describes a tamper detection circuit completed by a loop of wire which is the centre conductor of a coaxial cable. The electrical continuity of the centre conductor is thereby monitored. This arrangement prevents keeping the circuit intact with a simple shunt cable connected to the outer conductor of the coaxial cable while cutting the cable. However, two problems remain with this arrangement. Firstly, as electrical contacts with the cable are involved, the device is susceptible to electrical noise or being damaged by deliberate voltage spikes being applied to the cable. Secondly, it is still feasible that a thief could carefully peel back the outer sheath and central insulation of the device to expose the central conducting core. Shunt cables could then be provided by the thief for both inner and outer conductors of the coaxial cable so that the cable could then be cut while maintaining the electrical continuity of the tamper detection circuit.

[0009] The present invention aims to mitigate or solve one or more of the problems associated with the above-mentioned prior art devices.

[0010] Additionally or alternatively, the present invention aims to provide an electronic seal or system capable of/adapted to monitor/sense the integrity and/or continuity of (i) a closure member (e.g. an elongate member such as a cable, band, padlock hook, etc.) comprised in the seal or system and/or (ii) a security loop or other connection including/involving part or all of the closure member.

[0011] Additionally or alternatively, the present invention aims to provide an electronic security seal or system capable of communicating with a distant reading and/or programming device, for example capable of communicating the security status of the seal or system to the device.

First aspect of the invention

[0012] According to a first aspect of the present invention, there is provided an electronic seal comprising:

a housing;
a closure member cooperable with the housing to form a connection to close the seal,
the closure member comprising an outer portion enclosing one or more inner cores; and
means for sensing the integrity and/or continuity of some or all of the one or more inner cores.

[0013] The inventive seal has an advantage over the prior art Sealtronic and Electronic Seal PTE devices, which sense the electrical continuity of a standard cable, in that it is an inner core of the closure member rather than the whole of the closure member whose integrity/continuity is sensed. This means that it is more difficult for a thief to cut the cable without the tampering being detected. In particular, attaching a shunt cable to the outer portion of the closure member before cutting the closure member, to allow access to a container secured by the seal, would result in maintained continuity in the outer portion but a discontinuity in the inner core which would be detected; in contrast this procedure would avoid tamper detection in the Sealtronic devices as electrical continuity would be maintained by the shunt cable.

[0014] The closure member is preferably an elongate

member. This allows easy threading through a hole in a member to be secured by the seal (e.g. a hole in a lug in a container closure mechanism). Also, the present invention is more useful with an elongate member which is more likely to be cut (see below).

[0015] The outer portion is merely limited by its enclosing one or more inner cores, and can include a or the central axis (which can be curved) of the closure member or elongate member when this is not occupied by the one or more inner cores.

[0016] Preferably, the connection is formed by formation of a closed loop including part or all of the closure member. The loop can be any shape, not merely a curved shape. Two or more portions (e.g. end portions) of the closure member (e.g. elongate member) can be connected to the housing to form the loop.

[0017] In an alternative embodiment, when the connection is formed only one portion (e.g. an end portion) of the closure member (e.g. a rigid or flexible elongate member, e.g. a bolt or cable) is connected to the housing. The closure member here preferably comprises an enlarged head (e.g. bolt head) attached to one end of an elongate portion (e.g. shaft, shank, cable etc) of narrower cross-section containing the inner core(s), an opposing end of the elongate portion being adapted to be received (e.g. by means of a screw connection) by a recess of the housing. For example, the inner core(s) can comprise an optical fibre, one end of which is mirrored at the enlarged head, the other end of which is exposed at the opposing end of the elongate portion (e.g. bolt shaft/shank). Alternatively, the inner core(s) can comprise a conductor forming part of or connected to a capacitor, one end of the conductor being exposed at the elongate portion opposing end for electrical connection to the seal when connected. The sensing means is preferably disposed inside, and/or is fixed to, the housing so as to communicate with the inner core(s) when connected. Here, the bolt shank or other closure member elongate portion could pass through a hole in a lug to seal a container without a loop having been formed.

[0018] Preferably, the sensing means is for sensing (or during use senses) opening of the seal after closure of the seal. More preferably, the seal is for sensing (or during use senses) the integrity and/or continuity of the connection, the loop (if present) and/or a communication path or paths (e.g. optical path or electrical circuit) including (e.g. between) the sensing means and the sensed inner core(s). In this way, the seal is able to detect illicit opening of the seal effected by releasing the closure member without cutting it, as well as being able to detect cutting of or tampering with the closure member itself.

[0019] Preferably, the sensing means is disposed inside and/or fixed to the housing.

[0020] Preferably, the housing is engageable with one, two or more portions (e.g. end portions) of the closure member, such that the housing forms or encloses part of the loop when formed.

[0021] In one embodiment, one or more portions (e.g. an end portion) of the closure member are fixed to the housing, and the housing is engageable with an engaging portion (e.g. end portion) of the closure member.

[0022] Preferably, the housing comprises one or more recesses adapted to receive an end portion of the closure member.

[0023] Preferably, the housing comprises one or more locks adapted to lock one, two or more portions (e.g. one or two end portions) of the closure member in position when said portions are engaged with the housing. The one or more locks can comprise a sacrificial latching mechanism or a releasable lock or locks (e.g. a solenoid mechanism controlled by a microprocessor).

[0024] The one or more inner cores preferably extend along substantially all or most of the length of that portion of the closure member or elongate member which is disposed outside the housing when the seal is closed and which is included in the loop when formed. This substantially prevents the closure member or elongate member being cut without also cutting the inner core(s).

[0025] Preferably, the elongate member is flexible, but it can be rigid, e.g. in the form of a hook (as in a padlock hasp, for example).

[0026] Preferably, the elongate member comprises a cable.

[0027] Preferably, the outer portion of the cable or elongate member comprises metal (e.g. steel) wire or wires. More preferably, the outer portion comprises a plurality of inter woven strands of metal (e.g. steel) wire. This material imparts strength as well as flexibility.

[0028] In one embodiment, a single inner core is provided substantially coaxial with the outer portion of the closure member or elongate member.

[0029] In another embodiment, the elongate member (e.g. a cable) comprises a plurality of interwoven major strands (e.g. comprising metal wire), one, two or more of which being inner-core-containing major strands each of which comprises a major strand outer portion (e.g. comprising metal wire, e.g. a plurality of interwoven minor strands of metal wire) enclosing one of the one or more inner cores. Where two or more inner-core-containing major strands are provided, then the integrity/continuity of each inner core is sensed, i.e. sensing occurs at two cross-sectional positions of the elongate member so that tampering with/cutting the elongate member in a manner avoiding detection by the sensing means becomes even harder.

[0030] Some or all of the one or more inner cores can comprise an inner loop extending outward from a or the fixed portion of the closure member to at or near a or the engaging portion of the closure member and back to the fixed portion. This is particularly preferred where the closure member is an elongate member (e.g. comprising a cable) including a plurality of interwoven major strands (e.g. as described above), a first strand comprising one inner core forming the outward portion of the inner loop, and a second strand comprising one inner

core forming the backward portion of the inner loop. Remaining strands can be dummies containing inner cores not connected to the sensing means.

[0031] These embodiments are is harder to tamper with without detection as a person stripping the member does not know which strands are live and should be bypassed before cutting the member.

[0032] In an especially preferred embodiment of the invention, the one or more inner cores comprise one or more optical fibres, the sensing means comprises one, two or more optical detectors for sensing the integrity and/or continuity of some or all of the one or more optical fibres by detecting optical signals transmitted therealong, and the seal additionally comprises one, two or more optical sources for emission and transmission of optical signals into/along those of the one or more optical fibres which can be sensed. The optical detector(s) sense the optical properties of the optical fibre(s), which properties will change if the fibre(s) are cut or otherwise tampered with.

[0033] The above embodiment has the advantage that it is very hard to bypass the optical fibre core without changing the optical properties of the core radically, if such a bypass is possible at all. Tampering with or cutting the closure member is therefore almost always detected. This is favourably compared to the Dallas Semiconductor device in which the electrical continuity of the conducting core of the coaxial cable may be maintained by bypassing the core before cutting the cable (see above). A second advantage is that as there are no electrical contacts between the optical fibre(s) and the detector(s) or source(s), the seal is less susceptible to electronic noise or being damaged by deliberate voltage spikes being applied to the elongate member.

[0034] Preferably, the optical source(s) and/or optical detector(s) are part of the loop.

[0035] Preferably, the one or more optical fibres comprise an optical core of transparent optical material and an outer cladding enclosing the optical core. The transparent optical core preferably has a refractive index which varies from the inside to the outside of the optical core (e.g. a graded or stepped refractive index). This achieves internal reflection of an optical signal passing along. Preferably, the outer cladding comprises plastic (e.g. flexible plastic). The outer cladding is preferably opaque (e.g. black). The materials and methods of manufacture of the optical fibre are known to the skilled person.

[0036] Preferably, the ends of some or all of the one or more optical fibres are exposed at the surface of the closure member for communication with the optical detector(s) and/or optical source(s). Preferably, a first end of each optical fibre is exposed at a first end portion of the closure member and a second end of each optical fibre is exposed at a second end portion of the closure member.

[0037] Preferably, the seal comprises two means for both sensing and emitting optical signals (i.e. two combined optical sources/detectors) positioned for communication with opposing ends of some or all of the one or more optical fibres. This arrangement allows an optical signal to be transmitted in two directions along the relevant optical fibres, maximising the difficulty of detectionless tampering.

[0038] Whether or not optical fibres are used, the seal preferably comprises a microprocessor for receiving and processing data output by the sensing means relating to the integrity and/or continuity of the one or more inner cores (and preferably also relating to opening of the seal after closure) and for outputting said data and/or related data regarding the security status of the seal when required. The microprocessor is preferably suitable or adapted (e.g. via a suitable program) to receive and process the integrity/continuity data at different times, to compare each set of received data with one, some or all of the initial set or sets of integrity/continuity data obtained immediately after arming (or soon, e.g. 0-10 min e.g. 0-1min, thereafter), and to detect tampering by detecting a difference between the initial post-arming data and data received after tampering (e.g. that representing a significant change in the optical and/or electrical properties of the closure member).

[0039] The microprocessor preferably also controls the production of conditions required for the sensing means to sense the integrity and/or continuity of the core (s) (and preferably also opening of the seal) at different times (preferably at regular intervals). For example, where the one or more inner cores comprise one or more optical fibres and optical source(s) are present, the microprocessor controls optical signal emission from the optical source(s) into the optical fibre(s). The microprocessor may also control the lock(s).

[0040] Preferably, a clock is provided so that times of sealing/locking, arming, disarming, scanning by distant devices, and/or tampering may be detected.

[0041] Preferably, the microprocessor is connected to a memory for recording said integrity/continuity data. Preferably, the memory is suitable for recording a unique identification number of the seal, the contents of a container secured by the seal, the times and dates on which the seal was closed, locked and/or armed, and/or the times and dates on which tampering of the seal was detected.

[0042] The microprocessor can be programmed to take the actions which it is suitable for taking. A program can be provided for this purpose.

[0043] The microprocessor and other electrical components are preferably powered by an electrical power source, preferably a battery (e.g. a lithium battery for long life). The power source is preferably internal to the housing, and may be either permanently sealed within the housing or accessible and/or replaceable, e.g. by means of a removable cover allowing access to and replacement of the power source. Having a power source, the seal is able to continually sense its own security state, unlike passive transponder seals which are only

able to do so when they are energised by a scanning device.

[0044] Preferably, the seal comprises a transmitter controllable by the microprocessor and capable of receiving integrity/continuity data and/or related security status data from the microprocessor, said transmitter being able to transmit signals containing said data to a reading and/or programming device distant or separate from the seal.

[0045] The transmitter is preferably able to transmit signals comprising electromagnetic radiation, more preferably visible and/or infrared (IR) radiation. The use of visible/IR communication gives additional security from eavesdroppers when compared to radio frequency (RF). In addition, IR/visible radiation is much more directional than RF, being given out and received within a restricted cone, and this allows a distant reading device more easily to locate which IR/visible transmitting seal is transmitting where several such seals are present, or to distinguish between several such seals each transmitting simultaneously.

[0046] Preferably, the seal comprises a detector for detecting signals from a reading and/or programming device distant or separate from the seal. Preferably, for the same reasons as above, the detector is able to detect signals comprising electromagnetic radiation, more preferably visible and/or infrared radiation.

[0047] Preferably, the seal is programmed such that when armed the transmitter emits signals (e.g. beacon signals) intermittently, the signals preferably being emitted at regular intervals (e.g. of about 0.1 to 1 second), though signals at random intervals within a fixed (e.g. 0.8-1.2 sec) time range may enhance security in certain applications. The intermittent transmission saves power and the beacon signals allow a distant reading and/or programming device searching for the signal to synchronise with the seal.

[0048] Some or all of the intermittently transmitted signals usually comprise one, two or more consecutive pulses (e.g. each about 10 μs long). In some cases the number of pulses in each signal, or the time gap (e.g. 10-20 μs) between each pulse, may vary depending on whether the seal has been tampered with or not. In this way a suitably programed reading and/or programming device can detect the security status of the seal without responding to it.

[0049] If the seal then detects an acceptable password in a second signal from the device within a predetermined period after one of the intermittently-transmitted signals was emitted, the seal is preferably programmed to enter subsequently into continuous two-way communication with the device (e.g. emitting detailed security status data, container contents data, etc).

[0050] Preferably, the seal is programmed such that, when armed, the seal intermittently activates (e.g. at regular intervals e.g. of about 0.1 to 1 second), senses the integrity and/or continuity of the one or more inner cores (and preferably also opening of the seal), detects whether tampering has taken place, transmits via the transmitter one of the intermittently transmitted signals, searches for an acceptable response from the device, and then if no such response is detected deactivates until the next time for re-activation occurs. In this way, the armed seal spends most of its time de-activated, only activating briefly for self-sensing, tamper detection, transmission and searching. This saves power and prolongs the life of the power source (e.g. battery).

[0051] There is an alternative to using one or more optical fibres as the one or more inner cores of the closure member.

[0052] In this alternative embodiment, the one or more inner cores comprise one or more inner conductors connected or connectable to a terminal of an electrical power source, the one or more inner conductors being electrically insulated from each other and from the outer portion of the closure member;

the outer portion comprising a conductor connected or connectable to the opposing terminal of the power source;
the outer portion and the one or more inner conductors forming a capacitor or capacitors capable of storing charge provided by the power source;
and wherein the sensing means comprises a means for measuring charge and/or discharge characteristics of the capacitor or capacitors.

[0053] In this embodiment, the capacitance of the capacitor(s) depends on the length of the closure member. If the closure member were cut, then the charge/discharge characteristics of the member would change (e. g. the capacitance decreases, the decay/discharge curve changes, and the stored charge decays more quickly). The sensing means detects the change in the charge/discharge characteristics occurring during cutting.

[0054] One advantage that this embodiment has over the Dallas Semiconductor prior art device, which measures the electrical continuity of a conducting core of a coaxial cable, is demonstrated when a thief bypasses the conducting core(s) and the outer portion before cutting the cable (the closure member). In the prior art device, electrical conductivity may be maintained and detection may be avoided. In the present embodiment, bypass of the core(s) and outer portion would likely lead to a change in capacitance detectable by the sensing means.

[0055] Again, it is preferable that the closure member is an elongate member. This allows easy threading through a hole in a member to be secured (e.g. a hole in a lug in a container closure mechanism). A change in capacitance or discharge/charge characteristics is also more easily detectable when an elongate member is cut or tampered with.

[0056] Preferably, the means for measuring charge and/or discharge characteristics of the capacitor(s) is

adapted to measure the capacitor voltage remaining and/or the discharge current flowing at different times during discharge. The sensing means may measure the decay of the capacitor voltage during discharge.

[0057] The one or more inner conductors and the outer portion conductor are usually connected or connectable to their respective power source terminals indirectly, e.g. via an input/output device and/or a microprocessor.

[0058] Preferably, the microprocessor (e.g. as described above) of the seal comprises an input/output connector or connectors, connected or connectable to the capacitor(s), switchable between an output mode in which the capacitor(s) are charged up and an input mode in which the capacitor(s) are discharged into the microprocessor which senses the discharge characteristics of the capacitor(s).

[0059] Preferably, in the capacitance version of the invention, the inner conductor(s) and the conducting outer portion are connected or connectable to the power source via a portion (e.g. an end portion) of the closure member fixed to the housing, and the housing is engageable with an engaging portion (e.g. end portion) of the closure member.

[0060] The engaging portion of the closure member may be engageable with (e.g. slidably engageable within) a charge-storing portion of the housing such that the charge-storing portion contributes to the capacitance of the capacitor(s) when the engaging portion is so engaged. In this way, there will be a measurable change in capacitance if a thief releases the closure member (opens the seal) without cutting it.

[0061] The engaging end portion of the closure member or elongate member preferably carries a higher capacitance per unit length than that of the remaining portions of the closure member or elongate member. Thus, if the closure member or elongate member is cut near to the engaging end portion, the change in capacitance and charge/discharge characteristics will be significant and readily measurable by the sensing means.

Second aspect of the invention.

[0062] According to a second aspect of the present invention, there is provided a method of sensing the security status of an electronic seal according to the first aspect of the present invention, comprising the steps of:

(a) sensing the integrity and/or continuity of some or all of the one or more inner cores (and optionally also a communication path or paths including the sensing means and the sensed inner core(s)) at a certain time after closure and arming of the seal; and

(b) if the integrity and/or continuity of any of the sensed core(s) (or optionally the path or paths) has been compromised, recording that fact and/or that tampering has occurred.

[0063] Preferably, the method comprises the additional steps of:

(c) comparing the integrity and/or continuity data obtained in step (a) with previously recorded data representative of or obtainable from the sensed core or cores when in an integral state and optionally also from the sensed path or paths when continuous;

(d) detecting whether or not the data obtained in step (a) differs from the compared previously recorded data in a predefined manner and/or by more than a predefined extent; and

(e) if the data obtained in step (a) does so differ, recording that fact and/or that tampering has occurred and/or that the integrity/continuity has been compromised.

[0064] In step (c), the previously recorded data can comprise data with which the seal is provided without having been generated by self-sensing by the seal of the core(s) and optionally the path(s) (e.g. pre-programmed data).

[0065] Preferably, however, in step (c), the previously recorded data comprises that obtained at a defined preceding time after closure and arming of the seal.

[0066] In these ways, the method allows sensing of whether or not the properties (e.g. electrical and/or optical properties) of the closure member core(s), and optionally also the communication path(s), have changed significantly from when the seal was secured/closed and armed. Such a change will usually indicate tampering has occurred.

[0067] Preferably, in step (c), the previously recorded data comprises some or all of the initial set or sets of integrity/continuity data obtained immediately after arming or soon (e.g. less than 10 minutes or less than one minute) thereafter. This ensures that the basis for comparison is when the seal was in a secure untampered state.

[0068] Preferably, step (a) comprises sensing the integrity, continuity and/or optical properties of one or more optical fibres comprised in the one or more inner cores. This optical sensing method has the advantages of difficulty of by-passing and of low susceptibility to electronic damage as described above.

[0069] More preferably, step (a) comprises sensing the integrity, continuity and/or optical properties of one, two or more optical paths, each optical path including one of the one or more optical fibres, and an optical detector with which that optical fibre is in optical communication.

[0070] Optionally, some or all of the paths can include a medium between that optical fibre and the optical detector allowing said optical communication. The medium can comprise a body of gas (e.g. air) and/or one or more transparent solid materials (e.g. covering the detector). The optical detector is preferably part of the loop (if

present). In these ways, there is sensing not only of the integrity of the optical fibre(s) but also of the continuity of the optical path(s) or loop formed when the seal is closed. Therefore, not only cutting of or tampering with the closure member but also illicit opening of the seal without tampering with the closure member can be detected.

[0071] Even more preferably, step (a) comprises transmitting an optical signal from an optical source forming part of the seal into one portion (e.g. end portion) of some or all of the one or more optical fibres, and detecting whether or not a signal is received by the optical detector via another portion (e.g. end portion) of those fibre(s).

[0072] Two or more optical paths may be defined by two or more optical fibres communicating with the same optical detector.

[0073] In an alternative embodiment, step (a) comprises sensing the charge and/or discharge characteristics of a capacitor or capacitors comprised in the closure member.

[0074] The characteristics of the capacitor(s) can be as described hereinabove in the relevant embodiment of the seal.

[0075] Preferably, the method comprises measuring the capacitor voltage remaining and/or the discharge current flowing at different times during discharge. In this way, a decay curve is measured.

[0076] Preferably, the method comprises charging up the capacitor(s), and allowing the capacitor(s) to discharge while measuring the discharge characteristics of the capacitor(s).

[0077] Irrespective of which sensing embodiment is used, sensing the integrity/continuity can occur at regular intervals (e.g. of about 0.1 to 1 second).

[0078] Preferably, the method also comprises the seal transmitting signals intermittently to or for receipt by a reading and/or programming device distant or separate from the seal. The intermittent transmission saves power (e.g. maximising battery life).

[0079] Preferably, the intermittently-transmitted signals comprise beacon (guide) signals. These allow a distant reading and/or programming device searching for the signal to synchronize with the seal.

[0080] "Transmit" can include "emit" or "send out" without necessarily implying receipt by the device.

[0081] More preferably, the signals transmitted intermittently comprise electromagnetic radiation from a transmitter comprised in the seal.

[0082] Even more preferably, for additional security and directionality, the signals transmitted intermittently comprise visible and/or infrared radiation, and/or the transmitter is adapted to transmit visible and/or infrared radiation.

[0083] Preferably, the intermittently-transmitted signals are transmitted at regular intervals (e.g. of about 0.1 to 1 second). This aids synchronization. Alternatively, the intermittently-transmitted signals are transmitted at random or irregular intervals within a fixed time range (e.g. 0.8-1.2 sec); this may enhance security in certain applications).

[0084] Some or all of the intermittently-transmitted signals usually comprise one, two or more consecutive pulses (e.g. each about 10 μs long). In some cases the number of pulses in each signal, or the time gap (e.g. 10-20 μs) between each pulse, may vary depending on whether the seal has been tampered with or not. In this way a suitably programmed reading and/or programming device can detect the security status of the seal without responding to it.

[0085] Preferably, the method comprises activating the seal before steps (a) and (b) or (a) to (e), transmitting one of the intermittently transmitted signals, and deactivating the seal until the next time for re-activation occurs. This saves power. More preferably, the activation, sensing, transmission and de-activation occurs at regular intervals. This aids synchronisation by the distant reading and/or programming device.

[0086] Preferably, the method comprises searching for a second signal (e.g. in reply to one of the intermittently-transmitted signals) transmitted from the reading and/or programming device.

[0087] Preferably, for security and directionality, the searching step utilises a visible and/or infrared detector.

[0088] Preferably, the searching step takes place during a predetermined period after transmission of one of the intermittently-transmitted signals by the seal and before deactivation of the seal. More preferably, the searching step lasts 1 μs to 100 ms, more preferably 1 μs to 10 ms. This minimises the time during which the seal is activated, and saves power.

[0089] Preferably, if the second signal from the reading and/or programming device is detected, then the second signal received is recorded and/or if the second signal is acceptable deactivation is delayed until communication between the seal and the device is completed.

[0090] Preferably, the method of sensing includes receipt by the seal of a second signal from the device containing a password device, checking by the seal that the device password is acceptable, and subsequently transmitting a third signal containing password-protected data stored by the seal (e.g. security status data) from the seal to the device only if the password is acceptable. This is for security reasons. The data transmitted in the third signal is usually determined by the security level of the password received from the device.

[0091] Usually, the transmission of the third signal will form part of a continuous two-way communication between the seal and the device.

[0092] Preferably, the signals transmitted intermittently and/or the third signal is /are encrypted, e.g. using rolling encryption.

Third aspect of the invention

[0093] According to a third aspect of the present invention, there is provided an electronic seal comprising:

a housing;
a closure member cooperable with the housing to form a connection to close the seal; and a transmitter for transmitting signals containing data relating to the seal to a reading and/or programming device distant or separate from the seal.

[0094] Preferably, the seal comprises means for sensing the integrity and/or continuity of the closure member.

[0095] Preferably, the connection is formed by formation of a closed loop including part or all of the closure member. The sensing means is preferably for sensing opening of the seal after closure, more preferably for sensing the integrity and/or continuity of the connection, the loop (if present) and/or a communication path or paths including (e.g. between) the sensing means and the closure member.

[0096] Preferably, the closure member is an elongate member (e.g. comprising a cable).

[0097] The transmitter is preferably able to transmit signals comprising electromagnetic radiation, more preferably visible and/or infrared radiation. Visible/IR signals give additional security from eavesdroppers and are more directional than RF signals, as discussed above.

[0098] Preferably, the seal is programmed such that when armed the transmitter emits signals (e.g. beacon signals) intermittently, preferably at regular intervals (e. g. about every 0.1 to 1 second). This allows the device to synchronise with it and saves power.

[0099] Preferably, the seal is programmed such that when armed, the transmitter emits a third signal containing password-protected data (e.g. data relating to the security status of the seal, the time(s) of any tampering, container contents data, etc) only after receipt of a second signal from the device containing a password acceptable to the seal.

[0100] Preferably, the seal is programmed such that, when armed, the seal intermittently activates, senses the integrity and/or continuity of the closure member (and preferably also the path(s)), detects whether tampering has taken place, transmits via the transmitter one of the intermittently transmitted signals, searches for an acceptable response from the device, and then if no such response is detected deactivates until the next time for re-activation occurs. In this way, the armed seal spends most of its time de-activated, only activating briefly for self-sensing, detection and transmission. This saves power and prolongs the life of the power source (e.g. battery).

[0101] Preferably, the closure member comprises an outer portion enclosing one or more inner cores and the sensing means is for sensing the integrity and/or continuity of some or all of the one or more inner cores.

[0102] Other preferable features of the third aspect of the invention are as described hereinabove, being preferable features of the first aspect of the invention, all necessary changes being made.

Fourth aspect of the invention

[0103] According to a fourth aspect of the present invention there is provided a method of communication for a seal as defined in the first or third aspects of the invention comprising transmitting signals intermittently from a transmitter forming part of the seal to or for receipt by a reading and/or programming device distant or separate from the seal. This saves power (e.g. maximising battery life) compared to a continuous transmission.

[0104] "Transmit" can include "emit" or "send out" without necessarily implying receipt by the device or similar.

[0105] Preferably, the intermittently-transmitted signals comprise beacon signals (guide signals). These allow a distant reading and/or programming device searching for the beacon signals to synchronise with the seal.

[0106] Preferably, the intermittently-transmitted signals comprise electromagnetic radiation, more preferably visible and/or infrared radiation. Visible/ IR signals give additional directionality and security from eavesdroppers.

[0107] Preferably, the intermittently-transmitted signals are transmitted at regular intervals. This helps the device to synchronise with it.

[0108] Alternatively, the intermittently-transmitted signals may be transmitted at irregular or random intervals within a fixed time range (e.g. 0.8-1.2 sec).

[0109] Preferably, the signals are transmitted at intervals (regular or otherwise) of about 0.1 to 1 second. This is desirable to minimise power drain (which becomes significant for transmission at less than 0.1 second intervals) while also eliminating the risk of a dextrous thief opening and closing the seal between transmissions (which is possible for intervals of greater than about 1 second).

[0110] Some or all of the intermittently-transmitted signals usually comprise one, two or more consecutive pulses (e.g. each about 10 μs long). In some cases the number of pulses in each signal, or the time gap (e.g. 10-20 μs) between each pulse, may vary depending on whether the seal has been tampered with or not. In this way a suitably programmed reading and/or programming device can detect the security status of the seal without responding to it.

[0111] Preferably, the method comprises sensing the integrity and/or continuity of the closure member, detecting whether tampering has taken place, and then transmitting one of the intermittently-transmitted signals.

[0112] Preferably, the method comprises activating

the seal before transmission of one of the intermittently-transmitted signals (and optionally before sensing) and deactivating the seal after transmission. Even more preferably, the process is repeated several times, preferably at regular intervals (e.g. of about 0.1 to 1 second).

[0113] In this way, the armed seal spends most of its time de-activated, only activating briefly for self-sensing, detection and/or transmission. This saves power and prolongs the life of the power source.

[0114] Preferably, the method of communication includes transmitting a second signal (preferably an IR or visible signal) from the device to the seal (e.g. in reply to the seal), preferably during a predetermined period (e.g. 1μs-100ms, e.g. 1 μs-10ms) after transmission by the seal of one of the intermittently-transmitted signals and before deactivation of the seal.

[0115] More preferably, the second signal from the device to the seal contains a password of the device, and the method of communication includes checking by the seal that the device password is acceptable, and subsequently transmitting a third signal containing password-protected data stored by the seal (e.g. security status data) from the seal to the device only if the password is acceptable. This is for security reasons.

[0116] The data transmitted in the third signal is usually determined by the security level of the password received from the device

[0117] Usually, the transmission of the third signal will form part of a continuous two-way communication between the seal and the device.

[0118] Preferably, the third signal contains data relating to the seal.

[0119] Preferably, the third signal contains data relating to the security status of the seal (e.g. data regarding the integrity/continuity of the closure member, or data derived therefrom), and/or the time(s) of any tampering.

[0120] Alternatively or additionally, at the same or different times, the third signal can contain the time(s) of arming and/or locking of the seal, a seal identification number, and/or the contents of a container secured by the seal. Time(s) of reading of the seal by reading device (s) may also be transmitted.

[0121] Preferably, the intermittently-transmitted signals and/or the third signal is/are encrypted, e.g. using rolling encryption.

[0122] Other preferable features of the method of communication are as defined in the preferable or essential features of the other aspects of the invention, all necessary changes being made.

Fifth and Sixth aspects of the invention

[0123] According to a fifth aspect of the invention, there is provided a security system comprising

(i) an electronic seal according to the first or third aspects of the invention, and

(ii) an electronic reading and/or programming device distant or separate from the seal for communication with the seal.

[0124] According to a sixth aspect of the invention, there is provided an electronic reading and/or programming device suitable or adapted to (e.g. programmed to) communicate with a distant or separate electronic seal according to the first or third aspects of the invention.

[0125] Communication can be one-way in either direction, or two-way.

[0126] In the fifth or sixth aspects of the invention, the device can be a programming device (e.g. arming device) capable of arming or disarming the seal and/or locking or unlocking the seal. This programming device preferably is adapted to itself be disarmed on arming and/or locking of the seal by receipt of a signal from the seal which erases a password of the device, receipt and recognition of the device password by the seal being necessary to arm and/or lock the seal. This embodiment represents a cheap single-use item which can be widely distributed at goods distribution depots and is simple to use. Preferably, this type of device and the seal each have an outer conducting surface (e.g. sensor surface) capable of being brought into contact with each other so that signals can pass therebetween.

[0127] Preferably, the device is a reading device comprising a device detector for receiving transmissions from the seal and a device microprocessor for receiving and processing data relating to the security status of the seal. This allows distant/remote monitoring of the security status of the seal.

[0128] More preferably, the device is a reading and programming device which also comprises a device transmitter for transmitting signals to the seal, and wherein the device microprocessor is for controlling (e. g. arming or dis-arming) the seal via the device transmitter. This provides a versatile device capable of both controlling and monitoring the seal.

[0129] Most preferably, the device is programmed to search on instruction for beacon (guide) signals transmitted intermittently from the seal and, if such a signal is detected by the device detector, to transmit a second signal (e.g. including a password) via the device transmitter to the seal within a predetermined period after detection.

[0130] The device microprocessor can be programmed to take the actions which it is suitable for taking.

[0131] Preferably, the reading and/or programming device also includes input means (e.g. a keypad) for input of instructions by an operator of the device and/or output means (e.g. a display) for output of data to the operator.

[0132] Preferably, the device detector is able to detect visible and/or infrared radiation. Preferably, the device transmitter is able to transmit visible and/or infrared radiation. The use of IR/visible communication increases

security and directionality compared with RF.

[0133] Preferably, the reading and/or programming device has an electronic memory containing or recordable with a password and/or a unique device identification number for transmission to and/or recordal by the seal.

[0134] Preferably, the device comprises an information input means (e.g. a connector or detector) for receiving encrypted information from a remote computer. This allows the random generation of passwords and codewords by the (secure) remote computer and their transmission from the computer to the device without their being known to any human operators. This eliminates collusion.

[0135] Specific embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 is a cross- sectional view through a first embodiment of electronic seal in accordance with the present invention;

Fig. 2 is a perspective view of the electronic seal of Fig. 1, additionally illustrating a reading/programming device;

Fig. 3 is a perspective view of a coaxial cable forming part of the electronic seal of Fig. 1;;

Fig. 4 is a diagrammatic sectional view of the reading/programming device illustrated in Fig. 2;

Fig. 5 is a diagrammatic sectional view of an alternative construction of coaxial cable which can be used with the electronic seal of Fig. 1;

Fig. 6 is a cross-sectional view of a second embodiment of electronic seal in accordance with the present invention; and

Fig. 7 is a diagrammatic sectional view of an alternative construction of coaxial cable which can be used with the electronic seal of Fig. 6.

[0136] Fig. 1 shows an electronic seal 2 comprising a housing 4 and a flexible coaxial cable 6. Each of the two ends 7,9 of the cable 6 comprises a metal or plastic ferrule 7',9' crimped or bonded to the cable. Each ferrule 7',9' is substantially tubular and is of a greater external diameter than that of the cable, thereby forming an enlarged head at each end 7,9 of the cable 6.

[0137] One end of the housing 4, which may comprise plastic and/or metal, is provided with two spaced apart recesses 28, 30, each forming a socket for receipt of a respective one of the two cable ends 7,9, as shown in Fig. 1. The housing also contains means for securing the housing 4 to a body of a container or to a door or other closure closing an aperture to the container. The housing can be screwed or welded to the container or closure.

[0138] The housing 4 also contains a lock 12 comprising a sacrificial latching/locking mechanism adapted to lock each of the cable ends 7 and/or 9 in position when received within their respective recess 28,30. The lock 12 includes two lock members 12a, 12b reversibly movable between (i) a locked position, in which cable end 7 when received within recess 28 is locked in position by one lock member 12a and in which cable end 9 when received within recess 30 is locked in position by the other lock member 12b, and (ii) an unlocked position in which one or both of the ends 7,9 of the cable 6 can be moved into and out of their respective recesses 28 and /or 30.

[0139] The two lock members 12a, 12b comprise elongate bars movably mounted in a slot 12c in the housing 2 between the recesses 28,30, said elongate bars 12a, 12b being mounted and movable transversely to the longitudinal axis of their respective cable ends 7,9, each bar 12a, 12b including an outer end engageable with its respective cable ends 7,9 and an inner end 12d, 12e projecting outside the housing 4 to allow movement of the lock members 12a, 12b by hand. In the unlocked position, the inner ends 12d,12e of the lock members 12a, 12b abut each other (not shown). In the locked position (illustrated in Figs. 1 and 2), the inner lock member ends 12d, 12e are spaced apart to their maximum extent, exposing a gap therebetween.

[0140] A deformable elongate sacrificial lock member 12f (usually of rectangular or square cross section) is also provided, comprising two parallel elongate resilient legs 12g, 12h projecting in the same direction from the main portion thereof. The ends of the legs 12g, 12h are provided with laterally outwardly-projecting locking portions 12i, 12j adapted to latch into inwardly-facing undercuts 12k, 12L of the moveable lock member ends 12d, 12e. The lower (forward) faces 12m, 12n of the projecting leg portions 12i, 12j are upwardly/ rearwardly inclined relative to the legs 12g, 12h; this ensures that when the sacrificial member 12f is inserted into the gap between the moveable lock member ends 12d, 12e with the legs 12g, 12h forwardmost/innermost to the housing the legs 12g, 12h are deformed laterally inwardly to allow movement of sacrificial member 12f into the slot 12c, then springing outwards again when the projecting leg portions 12i, 12j are seated in the undercuts 12k, 12L.

[0141] The upper (rearward) faces 120, 12p of the projecting leg portions 12i, 12j (i.e. those faces which engage with undercuts 12k, 12L) are perpendicular (alternatively upwardly/rearwardly inclined) relative to the legs 12g, 12h; this ensures that the sacrificial lock member 12f is held within the slot 12c after insertion.

[0142] When inserted into the slot, the junction between the legs 12g, 12h and the main portion of the sacrificial member 12f is level with or marginally (e.g. 1 or 2 mm) higher than the top surfaces of the projecting ends 12d, 12e of the adjacent moveable lock members 12a, 12b. This allows "sacrificial" cutting of a leg when the lock member 12f is inserted but prevents the legs from being squeezed together which could otherwise allow the projecting leg portions 12i, 12j to be disengaged from their associated undercuts, thereby allowing removal of the lock member without cutting.

[0143] The sacrificial lock member 12f thereby prevents movement of the lock members 12a, 12b to the unlocked position and locks the seal 2. The lock 12 can only be released and the seal 2 can only be opened by cutting the sacrificial member 12f and removing the parts thereof from the gap between lock member ends 12d, 12e.

[0144] The flexible coaxial cable 6 has an outer sheath 8, formed from a plurality of woven (entwined) strands of steel wire (e.g. stainless steel or high-tensile steel) or formed from some other conventional material. The sheath 8 encloses a central core comprising an optical fibre 10,10A made of conventional materials (e.g. plastics such as polymethyl methacrylate or glass) and made using methods known to the skilled person. The optical fibre 10,10A comprises a transparent core 10 enclosed by a thin cladding layer 10A. The cladding 10A acts as a protective barrier material between the outer sheath 8 and the transparent core 10 of the optical fibre, and is black. The integrity of the optical fibre 10 can be checked at regular intervals by the seal 2 (see below).

[0145] At both ends 7,9 of the cable 6, the ends 11, 13 of the optical fibre 10 are exposed as shown in Fig. 3. When cable end 7 is fully received within recess 28, the optical fibre end 11 is in contact with and/or communicates with a first combined optical source and optical detector 14. When the end 9 of the cable 6 is fully received within recess 30, the optical fibre end 13 is in contact with and/or communicates with a second combined optical source and optical detector 16. This arrangement allows an optical signal or beam to be emitted by the first source/detector 14, transmitted in one direction via the fibre 10, and detected by the second source/detector 16, and vice versa. This allows sensing of the optical properties of the cable optical fibre 10, as described hereinafter. Alternatively, for uni-directional signal transmission, 14 can just be a source and 16 a detector, or vice versa. Bi-directional optical signal transmission maximises the difficulty of tampering.

[0146] Referring to Fig. 1, the housing 4 also contains a microprocessor 18, a read-only memory (ROM) 17 upon which is written a program for the microprocessor, a clock 21 and an erasable programmable read-only electronic memory (EPROM) 19. The memory 19 stores an identification serial number 15 (Fig. 2) unique to the seal 2 incorporating hidden check sums and/or passwords, and when the seal 2 is armed as will be described, the memory 19 records in encrypted and password-protected form information about the contents of the container being secured as well as the time of sealing and arming. The seal serial number 15 may also be printed on the outside of the seal housing 4.

[0147] The microprocessor 18 controls signal emission from, and monitors signal detection by, the optical sources/detectors 14,16 and on the basis of the emitted and/or received signals, determines the condition of the cable. The microprocessor 18 also records in memory 19 the processed security status data, and (optionally) controls the lock member 12 so as to secure or release one or both ends 7,9 of the cable 6. The microprocessor 18 also controls a beacon, transmitter or source 22 comprising a visible and/or infra-red (IR) transmitter, and a visible and/or infra-red detector 24, for two-way communication 35 with a separate external reading/programming device 40 (see later). Transmitter 22 and detector 24 are disposed within the housing 4 adjacent to an optical window 26, made of conventional materials, in the wall of the housing 4, such that visible and/or IR radiation can pass into and out of the housing to the detector 24 or from the transmitter 22.

[0148] The microprocessor 18, lock 12, source/detectors 14, 16, transmitter 22 and visible/IR detector 24 are powered by a battery 20. The battery 20 is internal to the housing 4, but alternatively could be located externally for some applications. The battery 20 is usually an alkaline battery for a high power output and for safety, though a lithium battery can be used for longer life. The battery may be permanently sealed within the housing 4 or alternatively may be removable via a removable cover in the housing allowing access to and replacement of the battery.

[0149] The various components of the electronic seal 2 are connected by electronic circuitry (e.g. a data bus) and via input/output devices (not shown) where appropriate (e.g. for the source 22 and detector 24) but since these are conventional they need not be described further.

[0150] The electronic seal 2 can communicate in two directions via its transmitter 22 and its detector 24 with a separate electronic reading and programming device 40, as shown in Figs. 2 and 4. This device 40 has a visible and/or infra-red transmitter 42 and an visible and/or infra-red detector 44, operated by a microprocessor 46 controlled by a suitable program held on ROM 56 and connected to an erasable programmable read-only memory 58 (holding a serial number unique to the device 40) and clock 60, and the whole connected by conventional circuitry and powered by a power source (e.g. a battery) 48. The device 40 also has a keypad 50 for input of data by the operator, and a visible display 52 for communication of output data to the operator, both connected to the microprocessor 46. Input/output means (eg. a connector or detector) 62 is provided for receiving and transmitting encrypted information 70 from or to a remote computer 80.

[0151] The seal 2 and reading/programming device 40 operate as follows, with particular reference to the use of the seal 2 to seal the door or shutter of a vehicle or container, which may contain valuable goods.

[0152] In use of the seal 2, after the vehicle or container has been loaded and the door or shutter closed, the cable 6 is passed through an aperture in a lug, projection, catch or other device used to fasten the door or shutter (not shown), so that the door or shutter cannot be opened without withdrawing or cutting the cable 6. The cable ends 7 and 9 are located fully within recesses

28 and 30 respectively and locked in position by means of the lock 12.

[0153] The seal 2 is armed and locked as follows. The reading/programming device 40 (either hand-held or attached to the wall of (e.g. a gatehouse) is brought within a few metres of the seal 2 (or vice versa). The operator directs the device window 54 towards the seal window 26 and actuates the keypad 50 (according to a set of instructions) to cause the microprocessor 46 to instruct the device's IR/visible transmitter 42 to send an IR and/or visible radiation signal, encrypted using rolling encryption, to the seal 2. This signal from the device 40 contains the unique serial number of the device 40 as well as a password accepted by the seal 2, instructions for the seal 2 to arm (and/or lock) itself, and information (typed in by the operator or otherwise provided) concerning the contents of the container sealed.

[0154] The signal passes through the optical window 26 of the seal 2, is detected by detector 24 and is translated and transmitted thereby to the seal microprocessor 18. The microprocessor 18 de-encrypts the signal, checks against its memory 19 to see if the received password is acceptable, and if so records the serial number of the device 40, the contents of the container and the time, causes the seal to arm itself and (if the lock 12 is a solenoid) the lock to engage the cable ends 7,9. The seal 2 then sends a return acknowledgement signal back to device 40, which records this.

[0155] According to one mode of sensing seal integrity, upon arming of the seal 2 the microprocessor 18 instructs each detector 14,16 to take a background reading at regular or pseudo-random intervals (e.g. every 1 second or thereabouts). Immediately after such a reading, the microprocessor 18 instructs each of the optical sources/detectors 14,16 to emit an optical signal along the fibre optic core 10 of the cable 6, and to thereafter take a second reading of any optical signal received from the other optical source/detector via the fibre optic cable 10. The background reading is subtracted from the second reading, to give a final reading which is compared with previous such readings. If acceptable final readings (i.e. similar to previous readings) are received by both detectors, the detectors inform the microprocessor 18 of this, which makes no record in its memory. If no signal (or a defective or indeterminate signal or a signal substantially different to those received before) is received from either detector, however, then the microprocessor 18 instructs the sources 14,16 to emit a second optical signal and the above procedure is repeated. If the same is a similar reading/signal is received then the optical fibre 10 or cable 6 or seal 2 has probably been tampered with and the processor 18 records in memory 19 (a) the time, (b) the detector(s) which received the defective/different optical signal and (c) that the security status of the seal is "tampered with".

[0156] An alternative mode of sensing seal integrity, which is particularly suitable for embodiments utilising fibre optic cores, involves emission of a time varying signal into the optical fibre 10 from the optical source 14. This time varying signal may simply be a pulsed signal. The microprocessor 18 monitors the output from the optical detector 16 in order to establish whether it receives a correspondingly time varying signal. In the event that it does not, the microprocessor 18 again records in the memory 19 the items a-c mentioned in the previous paragraph.

[0157] Whichever of the above described modes of integrity sensing is used, the seal 2 continues to self-check the integrity of the cable 6 every few seconds even after tampering, and if none or both detectors 14, 16 at some stage start to receive optical signals again, then the microprocessor 18 records the time and the detector in the memory 19, but the security status remains "tampered with".

[0158] Directly after each check of the integrity of the cable 6, the processor 18 instructs the transmitter 22 to emit an IR or visible beacon signal in encrypted and password-protected form. The beacon signal is emitted as one or a series of about 10 µs pulses at regular ca. 1 sec intervals (intermittently) directly after each seal self-checking operation.

[0159] After each self-checking operation and beacon transmission, the seal 2 shuts down, i.e., becomes dormant, until the regular time interval (e.g.,every 1 sec or so) elapses when the seal 2 reactivates to repeat the process. The seal 2 therefore is inactive for most of the time. This decreases power consumption and increases the life of the battery 20 and also the seal 2 itself if the battery is non-replaceable.

[0160] To interrogate the seal, the device 40 is brought to within a few metres of seal 2 and instructed to take a reading by the operator via keypad 50. The regular beacon signal from the seal 2 can then be read by the reading/programming device 40 via its detector 44, allowing location of and synchronisation with the seal 2, this fact being displayed via a display 52 or via a flashing LED (not shown). The reading device 40 then immediately (e.g. within 1µs to 10 ms, typically within 1 ms) emits an acknowledgement signal containing the or a device password and ID number which is detected and recorded by the seal 2. If the password is acceptable by the seal, the seal 2 then enters into a continuous two-way communication with the device 40 and transmits to the device 40 the data requested by it, the data transmitted depending on the security level of the device password received. This data can include the seal identification number 15, the contents of the container, the origin and/or destination, the time at which the seal was armed and/or locked; the security status of the seal 2, the time(s) of tampering (if any), the time(s) when the integrity of the optical fibre was re-established (if at all), and/or any other relevant information (e.g. time(s) of scanning by reading devices and/or their ID numbers, time interval between pulses, battery low, etc).

[0161] The seal 2 only needs to be active for a short time (e.g. a few milliseconds, e.g. 1 ms) after the beacon

signal to detect whether it has been read. If no device acknowledgment signal is received, or after any communications with the device are finished, the seal 2 shuts down until it is time for the next beacon.

[0162] In this way, the operator of reading device 40 can investigate the security status, et al, of the seal 2. The seal 2 records the fact that it has been scanned, the time of scanning, and the device ID number in memory 19.

[0163] The reading/programming device 40 can also instruct the seal 2 to disarm itself by transmitting a disarm password (and if applicable, also to unlock itself) when the container has reached its destination and/or to investigate the contents of the container if tampering has occurred.

[0164] When disarmed, the seal 2 is inactive (to maximise battery life). The seal 2 can be reused.

[0165] The seal 2 can be instructed to perform different actions by means of a hierarchy of different passwords, each password being for a specific instruction/action, e.g. arming, disarming, transmitting security status data or container contents, etc. Different devices 40 can be provided with differing arrays of passwords, thereby varying their functionality.

[0166] Passwords used in the currently preferred embodiments of the invention are 64 bits in length, so that obtaining the password by trial and error is exceedingly unlikely. The microprocessor may be programmed to require several passwords, each for a different activity - eg arming the seal, disarming the seal, reading the memory, writing to the memory, scanning seal integrity etc. In such a seal there may be provided a master password which is required in order to change the other passwords. Optionally, however, the microprocessor may be programmed to erase the contents of the memory upon receipt of the master password so that even if an unauthorised person obtains the master password, this still does not provide access to the contents of the memory.

[0167] The various passwords, code-words, and even the identification/serial numbers used by seal 2 and reading/programming device 40 may be generated at random and transmitted and read automatically by a secure computer network 70, 80 without being known to any human operators. This eliminates collusion and makes it more difficult for tampering with the seal to go undetected.

[0168] In alternative embodiments of the invention, seals and/or reading/programming devices are provided substantially identical to the seal 2 and device 40 described hereinabove, with the following modifications.

[0169] Firstly, modifications of seal 2 are considered. In one embodiment, the flexible coaxial cable 6 is replaced with a rigid member, e.g. a padlock hasp. The seal 2 can be a modified padlock.

[0170] In one alternative embodiment of seal 2 (not shown), one end (7 or 9) of the cable 6 is fixed to the housing 4 (no ferrule provided at that end), and the lock 12 and/or lock member(s) are adapted to lock the other releasable end (9 or 7) in position when received in its recess 28 or 30.

[0171] In another embodiment of seal 2, the sacrificial latching mechanism 12 is replaced with an internal solenoid mechanism which is locked simultaneously with arming of the seal 2 and which releases the cable 6 on receipt of a coded password from a microprocessor. This provides the seal with a releasable re-usable lock (no need to provide a new sacrificial part each time) but this consumes more power and so is most suitable to a large seal with a large battery attached to a vehicle. In a further embodiment sacrificial lock 12 is replaced with a releasable key-operated lock.

[0172] The sacrificial latching mechanism 12 may alternatively be replaced with a combination lock, operable manually. Such locks are of course well known. In such an embodiment the combination can optionally be recorded on the memory, access to the lock preferably being password protected.

[0173] In an alternative embodiment shown in Fig. 5, the flexible coaxial cable 6 of seal 2 is replaced with the flexible coaxial cable 6A comprising a plurality of interwoven (entwined) major strands 90. Two (alternatively more than two) of the major strands 90A, 90B comprise an outer sheath 92, e.g. formed from a plurality of interwoven minor strands of steel wire, enclosing a central core comprising an optical fibre 94, 94A of the same construction as optical fibre 10,10A (i.e. a cladding 94A enclosing a transparent core 94). Therefore each of the major strands 90A, 90B is of the same construction as cable 6. In this embodiment, more than one optical fibre 94, 94A is contained in a single coaxial cable 6A, and the integrity of each optical fibre is checked by the seal 2 (as described above), making this embodiment harder for a thief to tamper with without detection.

[0174] Alternative embodiments of the reading and programming device 40 are now discussed.

[0175] In one alternative inexpensive embodiment, device 40 may just be a reader, in which case it would only receive the intermittent beacon signal 5 via detector 44 transmitted by the transmitter 22 of seal 2. This beacon may include simple information as to whether or not the seal 2 has been tampered with.

[0176] In another embodiment (not shown), the reading and programming device 40 is replaced with an arming device, with a unique serial number and erasable memory and password, which is similar to device 40 but is adapted to arm the seal 2 by bringing the arming device up to the seal 2 (e.g. contacting the seal 2) and which arming device is adapted to itself be disarmed on arming the seal 2 by receipt of a signal from the seal 2 which erases the password of the arming device. The arming device is therefore a cheap single-use item which can replace the arming function of the reading/programming device 40. The seal 2 and arming device each have a conducting sensor surface (not shown) on the outside of their respective housings which can be brought into contact so that signals can pass in both di-

rections.

[0177] In this alternative embodiment, the seal 2 is armed by contacting the conducting sensor surface of the single-use arming device with the conducting sensor surface of the seal 2, or alternatively by IR/visible communication between the arming device and the seal 2. The arming device sends an electrical (or alternatively IR/visible) password protected and encrypted signal to seal 2, and the microprocessor 18 de-encrypts the signal , checks the password, records the device serial number and the time, and arms and/or locks the seal 2, as above. Additionally, when the seal 2 sends a return acknowledgement signal to the arming device, this has the effect of erasing the password of the arming device, so that the arming device can no longer be used. This single-use arming device is simple and cheaper than reading/programming device 40 and is therefore better adapted for wide distribution to all locations where the container will be sealed and dispatched, and for use by untrained operators. It also avoids possible abuse.

[0178] A second major embodiment of the invention is illustrated in Fig. 6. The embodiment is very similar to the previous embodiments in Figs. 1 to 3 and like features have been identified with like reference numerals, increased by 100. In this second major embodiment, an electronic seal 102 comprises a housing 104 containing microprocessor 118, erasable programmable read-only memory 119, clock 121, power source 120, and visible/IR transmitter 122 and visible/IR detector 124 adjacent optical window 126 similar to in Fig. 1. A flexible coaxial cable 106 is fixed at one end 107 to the housing 104 by a fixture 114, passes out through an opening 128 in the housing 104, and the other (releasable) end 109 is adapted to be received within a recess 130 and to be releasably locked in position therein by lock member or members of elongate lock 112.

[0179] In Fig. 6, the coaxial cable 106 comprises a coaxial cable in the form of a steel outer sheath 108, enclosing a central core 110 comprising a wire or other conductor capable of storing charge. The sheath 108 and core 110 are separated and electrically insulated from each other by a thin insulating tube 116. Core 110 terminates just before the releasable end 109 of the cable at a core end 113 encapsulated within and insulated (by tube 116) from the outer sheath 108. In this way, core 110 and sheath 108 together form a capacitor, the capacitance C of which depends on the length of the cable 106.

[0180] The fixed end 111 of the inner core 110 and the fixed end 107 of the outer sheath 108 are electrically connected by circuitry 135 to opposite terminals of an input/output device (e.g. pin) 136 of the microprocessor 118.

[0181] In operation, the releasable end 109 of the cable 106 is passed through an aperture in a lug or catch of the closure member of the container to be sealed, to prevent the closure member being opened, and disposed fully into recess 130. The seal 102 is locked and armed as described hereinbefore.

[0182] When the seal 102 is locked and armed, at regular intervals (approx every 1 second) the microprocessor 118 sets the input/output (I/O) device 136 to output a (say) 5 volt output which charges up the cable capacitor 108, 110 to a predetermined charge and voltage (defining the sheath as ground). A few microseconds later, after the capacitor is fully charged, the processor 118 resets the I/O device 136 to input mode and the cable capacitor 108, 110 discharges via the I/O device 136 into a second capacitor (not shown) inside the processor 118. The processor 118 measures how quickly the capacitor voltage V decays, i.e. measures a decay curve.

[0183] In general, the shorter the cable, the lower the capacitance C, and the quicker the voltage V decays. For known parameters of an intact cable, the decay curve will be predictable and either programmed into the processor 118 or measurable by the processor 118 immediately after arming or both.

[0184] The processor 118 makes charge-discharge measurements every one second or so and in this way self-checks the integrity of the cable 106 at regular intervals. As long as the decay curve remains the same, then the cable is unlikely to have been cut. However, if the cable 106 is tampered with, then the capacitance C of the cable will be affected, which will manifest itself in a different voltage decay as measured by the processor 118. This change is recorded by the processor 118 which refers to clock 121 and records in memory 119 that tampering occurred and at what time.

[0185] A small capacitor C1 (illustrated schematically in dotted lines) may also be connected between the releasable end 113 of the core 110 and the releasable end of the outer sheath 108. This gives the releasable end 109 of the cable 106 a significant capacitance, such that if the cable is cut near to that end 109, the change in capacitance will be significant, i.e. readily measurable by the processor 118.

[0186] In another variation of Fig. 6, the releasable end of the outer sheath 108, or a ferrule connected thereto, may be slidingly engageable with the walls of the recess 130, which walls are made of a conductor (e. g. metal) and which therefore form part of the total capacitance of the system when the cable 106 is engaged in the recess 130. In this way, there will be a measurable change in capacitance if a thief releases the cable 106 without cutting it.

[0187] In a further variation of Fig. 6, illustrated in Fig. 7, the flexible coaxial cable 106A comprises a plurality of (e. g. 5 or 6) woven (entwined) major strands 190. Two of the major strands 190A, 190B each comprise an outer sheath 192, e.g. formed from a plurality of woven minor strands of steel wire, enclosing a central conducting core 194. Core and sheath are separated by an insulating tube (not shown) as above. These two major strands 190A, 190B are integrally joined at the releasable end 109 of the cable 106A, i.e. together they comprise a single strand in the form of a loop 109A, 109B

extending from fixed cable end 107 to the releasable cable end 109 and then back to the fixed cable end 107. The remaining major strands 190 are dummies but still contain sheaths and central cores. This embodiment is even harder to tamper with without detection as a person stripping the cable does not know which strands are live and should be bypassed before cutting of the cable 106A.

[0188] The seal 102 can communicate with and be programmed with or read by a reading/programming device 40 or a single-use arming device as described hereinabove.

[0189] The invention is not restricted to the details of the foregoing embodiments.

Claims

1. An electronic seal (2) comprising a housing (4,104); a closure member (6,106) cooperable with the housing to form a connection to close the seal, the closure member comprising an outer portion (8,108) surrounding at least one core (10,110); and means (14,16,114) for sensing the integrity of the core.

2. An electronic seal as claimed in claim 1 wherein the core comprises an optical fibre (10,10A).

3. An electronic seal as claimed in claim 2 wherein the means for sensing the integrity of the core comprise an optical emitter (14) arranged to emit an optical signal into the core and an optical detector (16) arranged to detect a signal from the core.

4. An electronic seal as claimed in claim 3 wherein the optical emitter and optical detector are connected to control electronics (18) for causing the optical emitter to emit a time varying signal and for monitoring the output from the detector to establish whether a corresponding signal is received.

5. An electronic seal as claimed in claim 4 wherein the time varying signal is a pulsed signal.

6. An electronic seal as claimed in claim 1 wherein the core comprises at least one electrical conductor (110) connectable to a terminal of an electrical power source (136), the outer portion comprises an electrical conductor (108) which is connectable to the opposing terminal of the power source and is insulated from the core electrical conductor thereby providing a capacitance between the terminals of the power source, and the means for sensing comprises means (136,118) for measuring a characteristic of the capacitance.

7. An electronic seal as claimed in claim 6 wherein the closure member comprises a co-axial cable (106).

8. An electronic seal as claimed in any preceding claim comprising a microprocessor (18,118) for receiving and processing data output by the sensing means relating to the integrity of the core and for outputting said data when required.

9. An electronic seal as claimed in claim 8 wherein the microprocessor is connected to a memory (19,119) for recording said data.

10. An electronic seal as claimed in claim 8 or claim 9, further comprising a clock (21,121) so that times of sealing and/or tampering may be detected.

11. An electronic seal as claimed in claim 9 or claim 10 which is such that data relating to an item secured by the seal can be input to and retrieved from the memory.

12. An electronic seal as claimed in any of claims 8 to 11 which further comprises a transmitter (22,122) controllable by the microprocessor, said transmitter being capable of transmitting core integrity data to a remote reading device (40).

13. An electronic seal as claimed in claim 12 wherein the transmitter is for transmitting infra red signals.

14. An electronic seal as claimed in claim 12 or claim 13 which further comprises a detector (24,124) for detecting signals from a remote reading/programming device.

15. An electronic seal as claimed in claim 14 wherein the detector is for detecting infra red signals.

16. An electronic seal as claimed in claim 14 or claim 15 programmed such that when armed the transmitter emits signals intermittently.

17. An electronic seal as claimed in claim 16 programmed such that when armed the seal intermittently activates, senses the integrity of the core, transmits via the transmitter one of the intermittently transmitted signals, searches for an acceptable response from the reading device and then if no such response is detected deactivates until the next time for activation occurs.

18. An electronic seal as claimed in any of claims 14 to 17 programmed to require receipt of a password from the remote reading/programing device for at least selected activities.

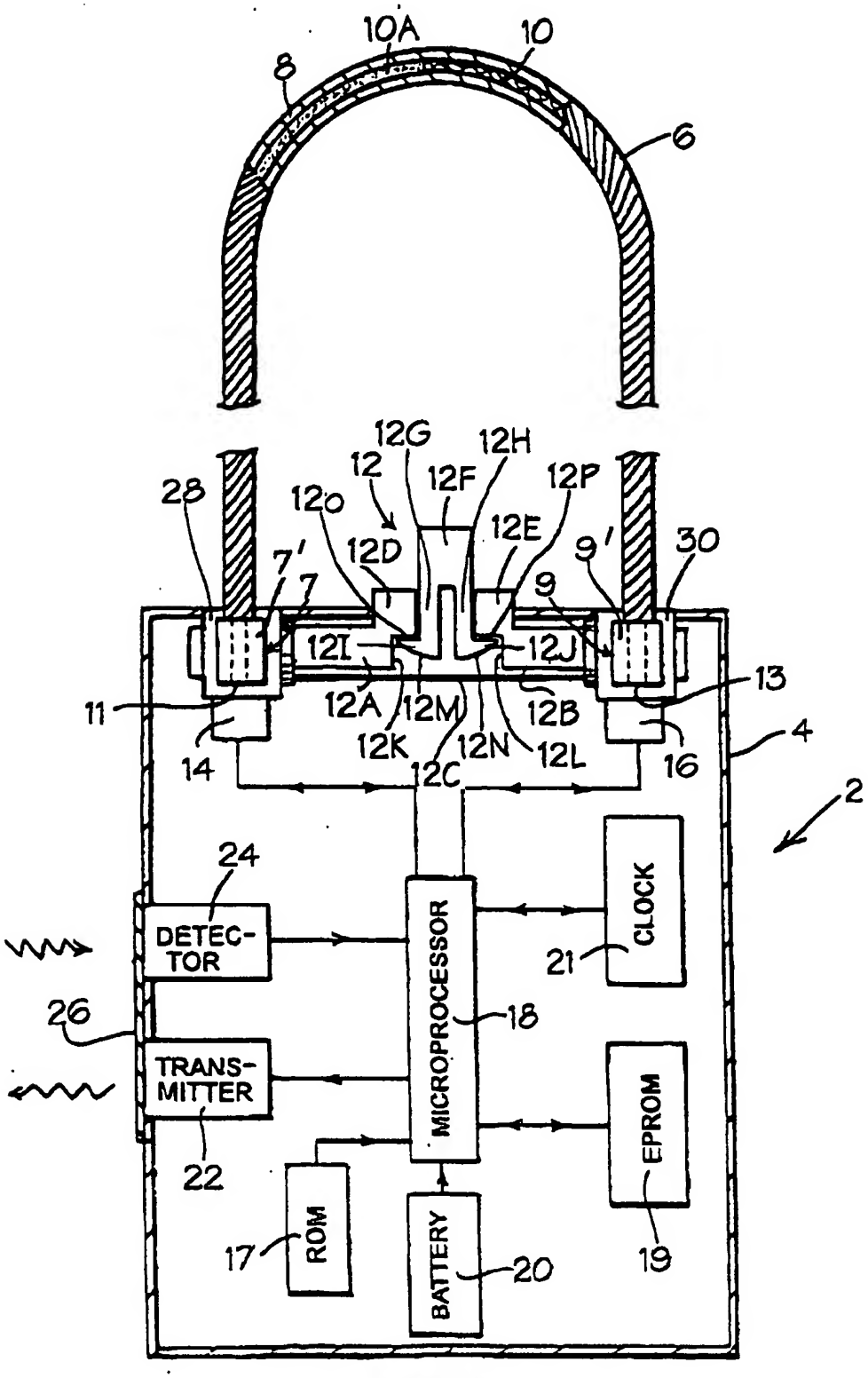
10A
10
8
6
12G
12H
12
12F
12P
28
12O
12E
12D
7'
9'
30
7
9
12I
12J
13
11
12A
12M
12B
12K
12N
12L
4
14
12C
16
2
24
DETEC-
TOR
CLOCK
21
26
MICROPROCESSOR
18
TRANS-
MITTER
EPROM
22
ROM
BATTERY
17
20
19

FIG 1

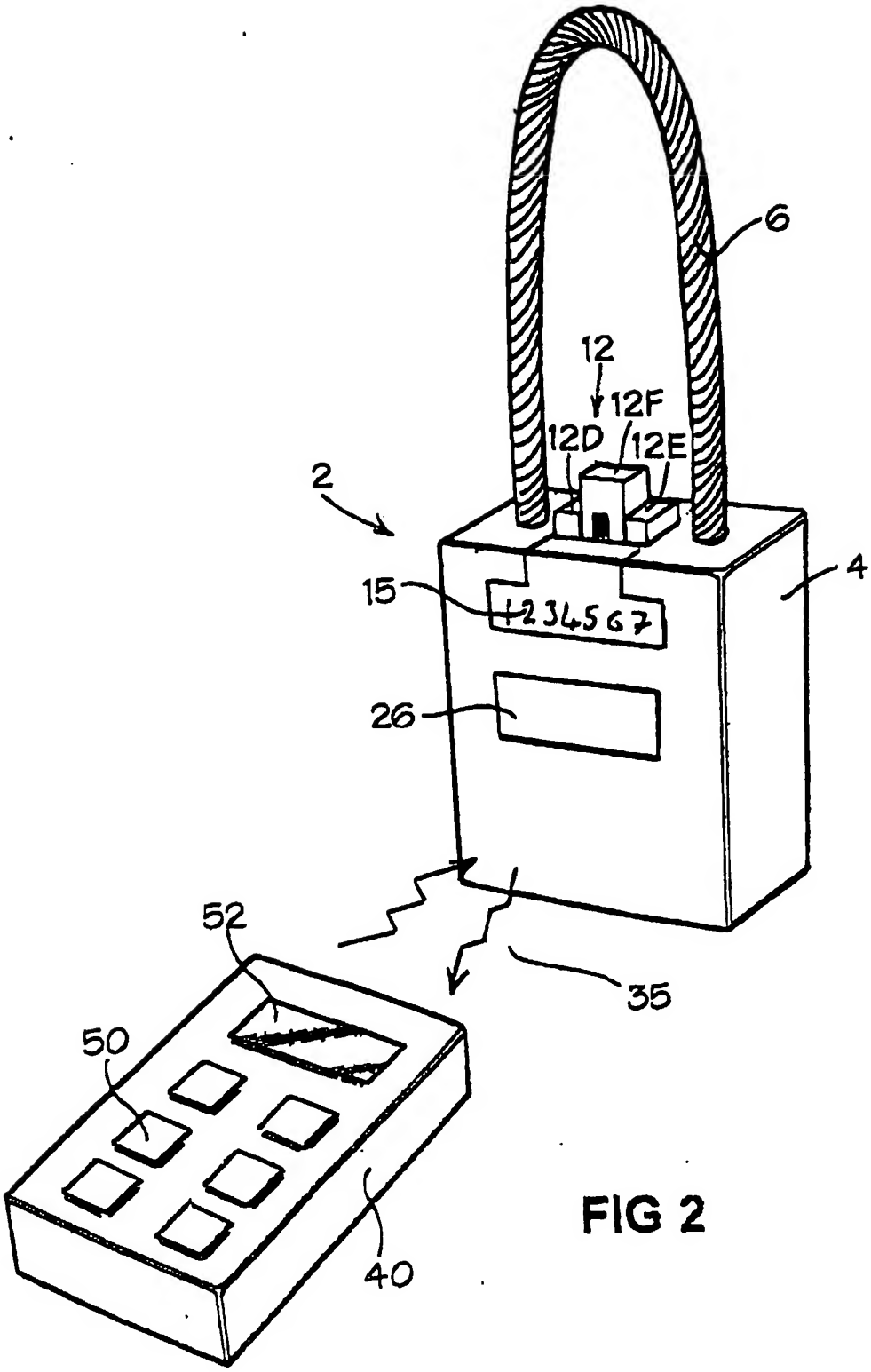

FIG 2

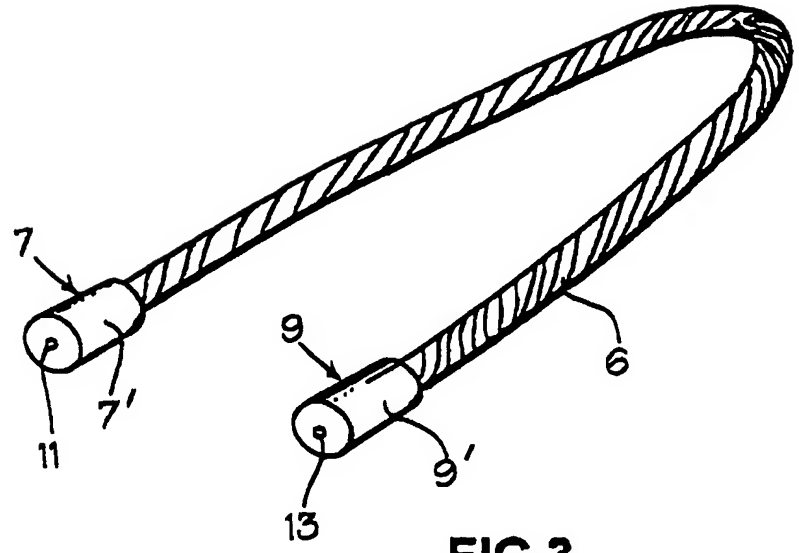
7
9
6
7'
11
9'
13

FIG 3

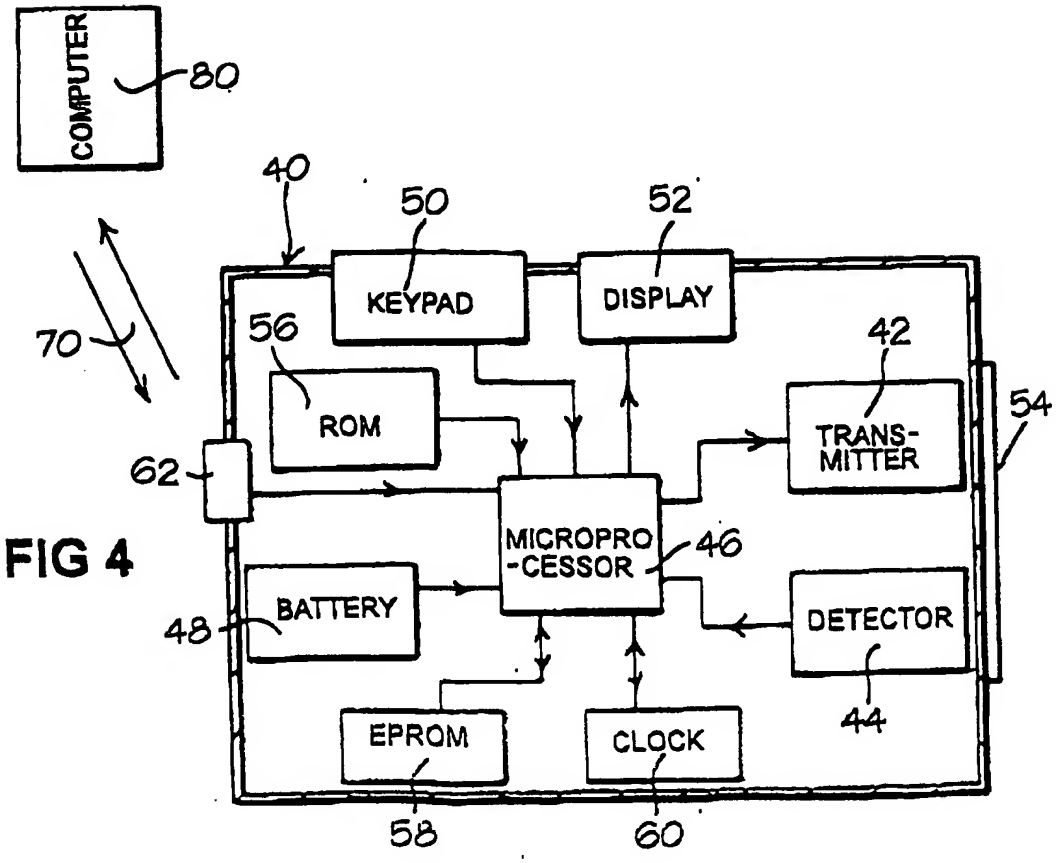
COMPUTER
80
40
50
52
KEYPAD
DISPLAY
70
56
42
ROM
TRANS-
MITTER
54
62
MICROPRO
-CESSOR
46
BATTERY
48
DETECTOR
44
EPROM
CLOCK
58
60

FIG 4

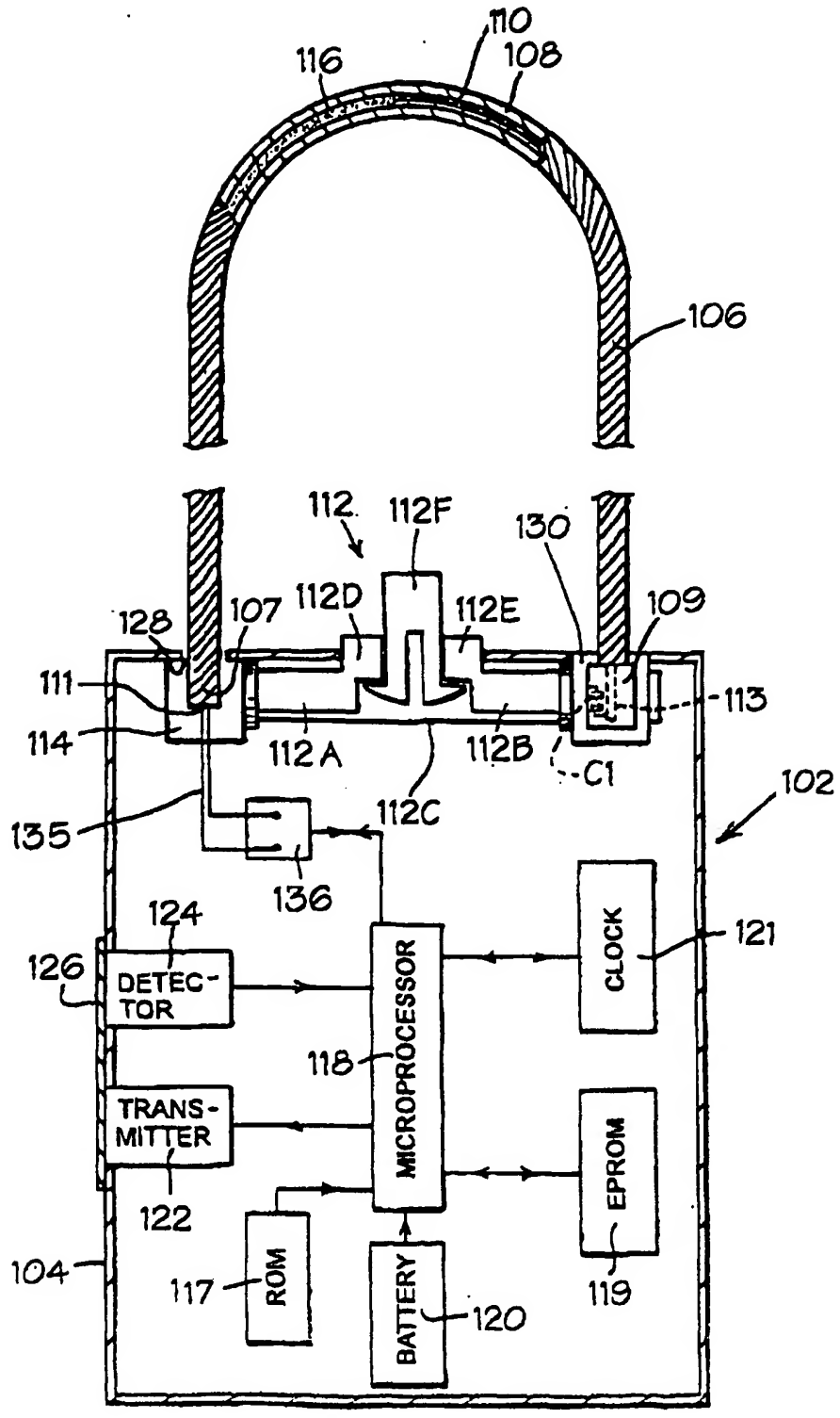
110
116
108
106
112
112F
130
112D
112E
109
128
107
111
113
114
112A
112B
C1
102
135
112C
136
124
126
DETEC-
TOR
MICROPROCESSOR
CLOCK
121
118
TRANS-
MITTER
EPROM
122
104
117
ROM
BATTERY
120
119

FIG. 6

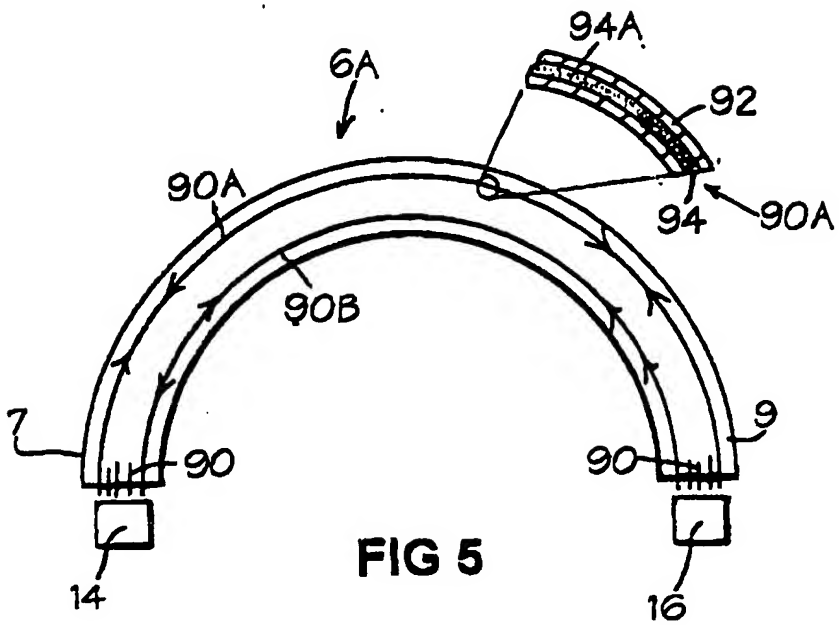
94A
6A
92
90A
94
90A
90B
7
90
90
9
14
16

FIG 5

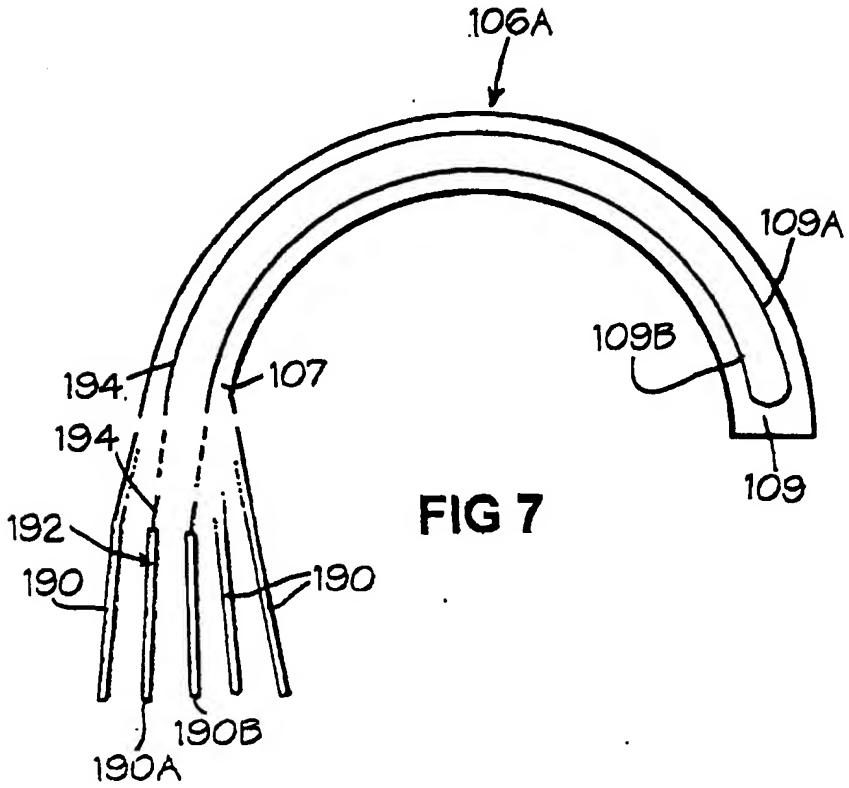
106A
109A
109B
194
107
194
109
192
190
190
190B
190A

FIG 7